REMARKS

Reconsideration is respectfully requested of the rejection of Claims 16-30 under 35 USC 101 as claiming the same invention as that of Claims 1-14 of prior US patent No 5,930,804.

Reconsideration is respectfully requested of the rejection of Claims 31-43 under 35 USC 101 as claiming the same invention as that of claims 1-15 of US patent No 6,182,076.

Reconsideration is respectfully requested of the rejection of Claims 16-43 under 35 USC 102 as being anticipated by Tabuki (US 5,706,427).

MPEP 804 in the definition of Double Patenting states that in determining whether a statutory basis for a double patenting rejection exists, the question to be asked is: Is the same invention being claimed twice? 35 USC 101 prevents two patents from issuing on the same invention. "Same invention" means identical subject matter. *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1984); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957). A reliable test for double patenting under 35 USC 101 is whether a claim in the application could be literally infringed without literally infringing a corresponding claim in the patent.

Pending claims 31-43 are drawn to a device (Claims 31-35) and an authentication system (claims 36-43). Issued claims 1-15 of US 6,182,076 include the claim limitation of at least one web server station linked to the Web cloud. None of Claim 31-43 includes such limitation, and a system that does not include a web station linked to the Web cloud as claimed in claims 1-15 of '706 may be literally infringing one of Claims 36-43 without literally infringe Claims 1-15 of '706.

It is therefore respectfully submitted that pending claims 31-43 could be literally infringed by a device that would not literally infringe Claim 1 of US 6,182,076 or any of its dependent claims 2-15. US 6,182,076 and pending claims 31-43 are therefore not drawn to the same invention and the statutory double patenting rejection of claims 31-43 is therefore incorrect and should be withdrawn.

The invention as claimed in Claim 31 relates to a device for enabling biometric authentication of an individual seeking access to a Web server from a Web client. The device compares live data received from the Web client. The live data correspond to biometric characteristic of the individual and the live data is correlated to at least one parameter received by the Web client. The parameter is characteristic of the live data transmitted by the Web client to the device.

The invention as claimed in Claim 36 relates to an authentication system for authenticating an individual seeking access to a web server from a web client. The system comprises among others a biometric device linked to the web client to provide live data respecting biometric characteristics of the individual. The live data is generated based on at least one parameter received by the Web client.

Tabuki relates to a system for authenticating users on a network. The system comprises a user host, a verification server and an application server. First the application server requests the user host to send authentication data, e.g. biometric physical quantity or digital signature. The user host in response to the request inputs the user's signature and sends this data to the verification server together with the identification data of the user (for example a membership number or a user name). The verification server saves the authentication data and identification data sent from the user host and verifies this against valid authentication data. That is, the verification server has an internal database with identification data for the identity claimed by the user host. The extracted authentication data and the authentication data received from the application server are compared and the verification result is sent back to the application server. (col.4, l.23-44).

Tabuki discloses the application server 10 requesting the user host 20 to send authentication data to a verification server. The user host 20, in response to the request, inputs the user's signature data from a tablet, and sends this data to the verification server 30. Tabuki does not disclose the user host receiving at least one parameter as claimed in the present invention and Tabuki also does not disclose the request transmitted to the host being or comprising a parameter characteristic of the live data (digital signature in Tabuki). In the invention, the parameter is for example one or more biometric characteristics for use in

authentication, with or without alternatives, a number of biometric characteristics to be used, without specifics as to which types can be used or as another example criteria for authentication including both selection among comparison algorithms and the confidence range or ranges for determining whether a sufficient match is obtained. Other examples of the parameter are given in the specification (see for example page 23)

The request received by the user host is not and does not comprise a parameter that is characteristic of the live data and Tabuki does not disclose the user host generating the live data based on the request or an element of the request characteristic of the live data. Claims 31 and 36 therefore clearly distinguish from Tabuki and the rejection of Claims 31-43 under 35USC102 should be withdrawn.

It is respectfully submitted that independent Claims 31 and 36 are patentable over Tabuki. It is also respectfully submitted that dependent Claims 32-35 and 37-43 are patentable over Tabuki at least based on their dependencies.

Applicants respectfully submit that they have answered all issues raised by the Examiner and that the application is accordingly in condition for allowance. Such allowance is therefore respectfully requested.

Please charge any fees other than the issue fee to deposit account 14-1270.

Please credit any overpayments to the same account.

Respectfully submitted,

Dated: May 21, 2003

By _____

Gwenaelle Le Pennec
Limited Recognition under 37 C.F.R 10.9(b)
(408) 617-4837